Desktop Management-Handbuch
Business PCs

Desktop Management-Handbuch

Business PCs

Erste Auflage (Juli 2007)

Dokumenten-Teilenummer: 451272-041

Allgemeines

Dieses Handbuch enthält Definitionen und Anleitungen zur Verwendung der Funktionen für Sicherheit und Manageability, die bei einigen Modellen voreingestellt sind.

⚠ **VORSICHT!** In dieser Form gekennzeichneter Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

△ **ACHTUNG:** In dieser Form gekennzeichneter Text weist auf die Gefahr von Hardwareschäden oder Datenverlust bei Nichtbefolgen der Anleitungen hin.

HINWEIS: In dieser Form gekennzeichneter Text weist auf wichtige Zusatzinformationen hin.

Inhaltsverzeichnis

1 Übersicht über Desktop Management

HP Client Management Solutions bietet auf Standards basierende Lösungen zur Verwaltung und Steuerung von Desktops, Workstations und Notebook-PCs in einer Netzwerkumgebung. HP war 1995 mit der Einführung der branchenweit ersten vollständig verwaltbaren Desktop-PCs ein Vorreiter im Bereich der Desktop Manageability. Die Manageability-Technologie von HP ist patentrechtlich geschützt. Seither ist HP führend bei der Entwicklung der Normen und Infrastruktur, die für eine effektive Nutzung, Verwaltung und Konfiguration von Desktops, Workstations und Notebooks erforderlich sind. Dabei entwickelt HP eigene Management-Software und arbeitet eng mit marktführenden Anbietern von Management-Software-Lösungen zusammen, um die Kompatibilität zwischen HP Client Management Solutions und diesen Produkten sicherzustellen. HP Client Management Solutions ist ein wichtiger Bestandteil der umfassenden HP Lösungen, mit denen sich die Betriebskosten senken und die Manageability Ihrer PCs während des gesamten Lebenszyklus gewährleisten lassen.

Die zentralen Funktionen und Merkmale des Desktop Management lauten:

- Erstkonfiguration und -einsatz
- Remote System Installation
- Software-Aktualisierung und -Management
- ROM-Flash
- Konfiguration optionaler Hardware-Geräte
- Bestandsüberwachung und Sicherheit
- Fehlermeldung und -beseitigung

HINWEIS: Die Unterstützung spezieller, in diesem Handbuch beschriebener Funktionen kann je nach Modell oder Softwareversion variieren.

2 Erstkonfiguration und -einsatz

Der Computer wird mit einem vorinstalliertem Systemsoftware-Image ausgeliefert. Nach einem kurzen Entpackvorgang ist der Computer einsatzbereit.

Möglicherweise ziehen Sie es vor, das vorinstallierte Software-Image durch eine benutzerdefinierte System- und Anwendungssoftware zu ersetzen. Es gibt mehrere Methoden zum Ersetzen eines benutzerdefinierten Software-Images. Folgende Methoden können verwendet werden:

- Installation zusätzlicher Software-Anwendungen nach dem Auspacken des vorinstallierten Software-Images
- Verwendung von Software-Bereitstellungs-Tools wie HP OpenView Client Configuration Manager (derzeit nicht für Windows Vista verfügbar), HP OpenView PC Configuration Management Solution (basierend auf Radia-Technologie; derzeit nicht für Windows Vista verfügbar) oder Altiris Deployment Solution, um die vorinstallierte Software durch ein benutzerdefiniertes Software-Image zu ersetzen.
- Verwendung eines Disk-Cloning-Vorgangs zum Kopieren des Inhalts einer Festplatte auf eine andere

Welches Einsatzverfahren am besten geeignet ist, hängt von Ihrer IT-Umgebung und den damit verbundenen Prozessen ab. Im Abschnitt über den PC-Einsatz auf der HP Lifecycle Service-Website (http://h20219.www2.hp.com/services/cache/80906-0-0-225-121.html) finden Sie Informationen zur Auswahl des geeigneten Einsatzverfahrens.

Die *Restore Plus!* CD, das ROM-basierte Setup und die Hardware mit ACPI-Unterstützung bieten zusätzliche Hilfe bei der Wiederherstellung der Systemsoftware, dem Konfigurationsmanagement, der Fehlerbeseitigung und der Energieverwaltung.

HINWEIS: Unter „HP Backup and Recovery Manager“ auf Seite 10 finden Sie weitere Informationen zur Erstellung der *Restore Plus!* -CD.

HP OpenView Agent

HINWEIS: HP OpenView Agent ist derzeit nicht für Windows Vista verfügbar.

Der von HP OpenView Client Configuration Manager und HP OpenView PC Configuration Management Solution verwendete Management-Agent ist auf Ihrem Computer vorhanden. Wenn er installiert wird, ermöglicht er die Kommunikation mit der HP OpenView Management-Konsole.

So installieren Sie HP OpenView Agent:

1. Klicken Sie auf **Start**.
2. Klicken Sie auf **Alle Programme**.
3. Klicken Sie auf **HP Manageability**.
4. Klicken Sie auf **Radia Management Agent Readme**.
5. Lesen und befolgen Sie die Anleitungen der Readme-Datei, um HP OpenView Agent zu installieren.

HP OpenView Agent ist eine zentrale Infrastrukturkomponente für die Aktivierung der gesamten HP OpenView PC Configuration Management Solution. Ausführliche Informationen zu den anderen Infrastrukturkomponenten, die für den Einsatz der HP OpenView PC Configuration Management Solution erforderlich sind, finden Sie unter http://h20229.www2.hp.com/solutions/ascm/index.html.

Altiris Deployment Solution Agent

Dieses Programm ist auf Ihrem Computer vorhanden. Wenn es installiert wird, ermöglicht es die Kommunikation mit der Deployment Solution-Administratorkonsole.

So installieren Sie Altiris Deployment Solution Agent:

1. Klicken Sie auf **Start**.
2. Klicken Sie auf **Alle Programme**.
3. Klicken Sie in Windows Vista auf **Altiris Dagent installieren**.

   Klicken Sie in Windows XP auf **Altiris AClient installieren**.
4. Folgen Sie den Anleitungen auf dem Bildschirm, um den Altiris-Client einzurichten und zu konfigurieren.

Altiris Deployment Solution Agent ist eine zentrale Infrastrukturkomponente für die Aktivierung der Client Foundation Suite und der Client Premium Suite von HP. Ausführliche Informationen zu den anderen Infrastrukturkomponenten, die für den Einsatz der HP Client Foundation Suite und der Client Premium Suite erforderlich sind, finden Sie unter http://www.hp.com/go/easydeploy.

3 Remote System Installation

Mit Remote System Installation können Sie das System mit Hilfe der Software und der Konfigurationsdaten von einem Netzwerkserver aus starten und installieren. Hierfür wird Preboot Execution Environment (PXE) gestartet. Die Remote-Installationsfunktion wird normalerweise als Tool zur Systemeinrichtung und -konfiguration verwendet. Sie kann darüber hinaus für folgende Aufgaben eingesetzt werden:

- Formatieren einer Festplatte
- Verwenden eines Software-Images auf einem oder mehreren neuen PCs
- Remote-Aktualisierung des System-BIOS im Flash-ROM („Remote ROM Flash“ auf Seite 15)
- Konfigurieren der BIOS-Einstellungen des Systems

Zum Starten von Remote System Installation drücken Sie F12, sobald beim Hochfahren des Computers in der rechten unteren Ecke der HP Logoanzeige die Meldung **F12 = Network Service Boot** (Starten über Netzwerk) erscheint. Folgen Sie den Bildschirmanleitungen, um fortzufahren. Die standardmäßige Startreihenfolge ist eine BIOS-Konfigurationseinstellung, die jedoch so geändert werden kann, dass stets ein PXE-Startvorgang erfolgt.

4 Software-Aktualisierung und -Management

HP stellt eine Reihe von Tools für die Verwaltung und Aktualisierung von Software auf Desktops, Workstations und Notebooks zur Verfügung:

- HP Client Management Interface
- HP System Software Manager
- HP Client Manager
- HP ProtectTools Security Manager
- HP Client Premium Suite
- HP Client Foundation Suite
- HP OpenView Agent Client Configuration Manager (derzeit nicht für Windows Vista verfügbar)
- HP OpenView PC Configuration Manager Solution (derzeit nicht für Windows Vista verfügbar)
- HP Client Catalog for SMS
- HP Backup and Recovery Manager
- Intel vPro-PCs mit Active Management Technology
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Unabhängig von den Systemverwaltungstools, die Ihre IT-Abteilung verwendet, ist eine effiziente Verwaltung von Hardware und Software extrem wichtig, um Ihre IT-Kosten niedrig und das Unternehmen flexibel zu halten. Der IT-Administrator kann auf die HP Client Management Interface zugreifen, indem er einfache Skripte schreibt und diese Skripte in die gewünschte Management-Lösung integriert.

Mit HP Client Management Interface (HP CMI) lassen sich neue HP Business PCs nahtlos in eine verwaltete IT-Umgebung einbinden. HP CMI bietet eine Schnittstelle für die einfache Integration von HP Business PCs in gängige Systemverwaltungstools wie Microsoft Systems Management Server, IBM Tivoli Software und HP OpenView Operations sowie proprietäre Managementanwendungen. Mit HP CMI können Tools und Anwendungen für das Systemmanagement detaillierte Client-Inventardaten und Informationen über den Festplattenstatus abrufen sowie BIOS-Systemeinstellungen verwalten, indem sie direkt mit dem Client-Computer kommunizieren. Auf diese Weise lässt sich bei einem deutlich geringeren Bedarf an Agenten- oder Anschluss-Software eine effektive Integration erzielen.

HP Client Management Interface basiert auf Industriestandards wie Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) und Advanced Configuration and Power Interface (ACPI). HP CMI ist eine Basistechnologie, die bei HP Client Management Solutions eingesetzt wird. Mit HP CMI erhalten Sie die notwendige Flexibilität, um selbst zu entscheiden, wie Sie Ihre HP Client-Computer verwalten möchten.

In Kombination mit Systemverwaltungssoftware bietet HP Client Management Interface folgende Vorteile:

- Bereitstellung detaillierter Client-Inventardaten – Erfassung ausführlicher Informationen zu Prozessoren, Festplatten, Speicher, BIOS und Treibern einschließlich Messdaten wie Lüfterdrehzahl, Spannung und Temperatur.
- Bereitstellung von Informationen zum Festplattenstatus - Auswahl aus einer breiten Palette an Warnmeldungen zur Client-Hardware (z. B. Überhitzung, Lüfterausfall und Änderungen der Hardware-Konfiguration), die an die Systemverwaltungskonsole, die Anwendung oder den lokalen Client-Computer gesendet werden können. Dabei werden die Warnmeldungen bei Auftreten entsprechender Hardware-Ereignisse in Echtzeit übertragen.
- Verwaltung von BIOS-Systemeinstellungen – Durchführung von F10-Funktionen wie Einrichten und Ändern von BIOS-Kennwörtern sowie Remote-Definition und -Änderung der Startreihenfolge für beliebige Client-Systeme über die Systemverwaltungskonsole

Weitere Informationen zu HP Client Management Interface finden Sie unter http://www.hp.com/go/hpcmi/.

HP System Software Manager

HP System Software Manager (SSM) ist ein kostenloses Dienstprogramm, das die automatische Remote-Bereitstellung von Gerätetreibern und BIOS-Updates für vernetzte HP Business PCs ermöglicht. SSM ermittelt im Hintergrund (d. h. ohne Benutzerinteraktion) die Treiber- und BIOS-Version auf dem vernetzten Client-System und vergleicht diese Daten mit Systemsoftware-SoftPaqs, die getestet und in einem zentralen Dateiarchiv abgelegt wurden. Danach ersetzt SSM veraltete Systemsoftware auf den vernetzten PCs automatisch durch die betreffende aktuelle Version aus dem Archiv. Da SSM absolut zuverlässig dafür sorgt, dass nur die richtigen SoftPaq-Updates auf die jeweiligen Client-Systemmodelle aufgespielt werden, können Administratoren mit diesem Dienstprogramm ihre Systemsoftware sicher und bequem auf dem neuesten Stand halten.

System Software Manager arbeitet reibungslos mit Tools für die Verteilung von Unternehmenssoftware zusammen, zu denen z. B. HP OpenView PC Configuration Management Solution (derzeit nicht für Windows Vista verfügbar), Altiris HP Client Manager und Microsoft Systems Management Server (SMS) gehören. SSM ermöglicht die komfortable Verteilung von Updates, die vom Kunden generiert oder von Dritten bereitgestellt und im SSM-Format gepackt werden.

SSM kann kostenlos unter folgender Adresse heruntergeladen werden: http://www.hp.com/go/ssm.

HINWEIS: SSM unterstützt derzeit keinen Remote-ROM-Flash auf Systemen mit aktiviertem Windows Vista BitLocker, die TPM-Maßnahmen zum Schutz der BitLocker-Schlüssel verwenden. Ein Flash des BIOS würde dazu führen, dass die von BitLocker für die Plattform erstellte Vertrauenssignatur ungültig wird. Aktivieren Sie BitLocker über die Gruppenrichtlinien, um ein Flash des System-BIOS herbeizuführen.

Sie können BitLocker-Unterstützung ohne TPM-Maßnahmen des BIOS aktivieren, um zu verhindern, dass die BitLocker-Schlüssel ungültig werden. HP empfiehlt, dass Sie ein sicheres Backup der BitLocker-Zugangsdaten aufbewahren, damit Sie notfalls schnell wiederherstellen können.

HP Client Manager

Der gemeinsam mit Altiris entwickelte HP Client Manager steht kostenlos für alle unterstützten HP Business Desktop-, Notebook- und Workstation-Modelle zur Verfügung. Über die integrierte SSM-Funktionalität ermöglicht HP Client Manager die zentrale Hardware-Erfassung, -Überwachung und -Verwaltung für HP Client-Systeme.

HP Client Manager zeichnet sich durch folgende Merkmale aus:

- Bereitstellung nützlicher Hardware-Informationen zu CPU, Speicher, Videosystem und Sicherheitseinstellungen
- Überwachung des Systemzustands für die proaktive Behebung potenzieller Probleme
- Automatisches Aufspielen und Installieren von Treiber- und BIOS-Updates, ohne dass der Administrator tatsächlich vor Ort sein muss
- Fernkonfiguration von BIOS- und Sicherheitseinstellungen
- Automatisierung von Prozessen für eine schnelle Behebung von Hardwareproblemen

Enge Einbindung in HP Instant Support Tools für die schnellere Behebung von Hardwarefehlern

- Diagnostics – Remote-Ausführung und -Anzeige von Berichten zu HP Desktop-, Notebook- und Workstation-Modellen
- System Health Scan – Überprüft die installierten HP Client-Systeme auf bekannte Hardwareprobleme
- Active Chat – Stellt eine Verbindung zur HP Kundenunterstützung her
- HP Knowledgebase – Bietet eine Fülle von wertvollen Tipps und Informationen
- Automatischer SoftPaq-Abruf- und Bereitstellungsprozess für die schnelle Behebung von Hardwareproblemen
- Erkennung, Inventarisierung und Initialisierung von Systemen mit dem integrierten Sicherheitschip von HP ProtectTools
- Optionale Ausgabe von Warnmeldungen zum Systemzustand auf lokalem Client-System
- Protokollierung grundlegender Inventardaten für nicht von HP stammende Clients
- Einrichten und Konfigurieren des TPM- Sicherheitschip
- Zentrales Planen der Client-Sicherung und Wiederherstellung
- Zusätzliche Unterstützung für die Verwaltung von Intel AMT

Weitere Informationen zu HP Client Manager finden Sie unter http://www.hp.com/go/clientmanager.

HP ProtectTools Security Manager

Die ProtectTools Security Manager Software stellt Sicherheitsfunktionen zur Verfügung, die Schutz vor dem unberechtigten Zugriff auf Computer, Netzwerke und kritische Daten bieten. Dabei ist durch die folgenden Module eine optimale Sicherheit gewährleistet:

- Smart Card Security for ProtectTools
- Embedded Security for ProtectTools

- BIOS Configuration for ProtectTools
- Credential Manager for ProtectTools

Welche Module für Ihren Computer zur Verfügung stehen, ist vom jeweiligen Modell abhängig. So muss für Embedded Security for ProtectTools z. B. der integrierte Trusted Platform Module (TPM) Sicherheitschip auf Ihrem Computer installiert sein (nur bestimmte Modelle), während Smart Card Security for ProtectTools eine optionale Smart Card und ein entsprechendes Lesegerät benötigt.

Die ProtectTools-Module können vorinstalliert bzw. auf der Festplatte vorhanden sein, oder Sie können sie auf der HP Website bestellen. Weitere Informationen hierzu finden Sie unter http://www.hp.com/products/security.

HP Client Premium Suite

Die HP Client Premium Suite (HP CPS) ist für Unternehmen ausgelegt, die den gesamten Lebenszyklus ihrer Client-Hardware und -Software von einer zentralen, webbasierten Managementkonsole aus verwalten möchten. Sie besteht aus folgenden Modulen:

- HP Client Manager
- HP Systems Insight Manager Connector
- HP OpenView Connector (derzeit nicht für Windows Vista verfügbar)
- Altiris Client Manager Suite – Level 1
- Altiris Connector Solution
- Altiris Local Recovery Pro
- Altiris AuditExpress

Weitere Informationen zur HP Client Premium Suite finden Sie unter http://www.hp.com/go/easydeploy.

HP Client Foundation Suite

Die HP Client Foundation Suite (HP CFS) richtet sich an Unternehmen, die grundlegende Funktionen für die Client-Verwaltung benötigen. Sie besteht aus folgenden Modulen:

- HP Client Manager
- HP Systems Insight Manager Connector
- Altiris Migration Suite
- Altiris Local Recovery Pro

Weitere Informationen zur HP Client Foundation Suite finden Sie unter http://www.hp.com/go/easydeploy.

HP OpenView Client Configuration Manager

HINWEIS: HP OpenView Client Configuration Manager ist derzeit nicht für Windows Vista verfügbar.

HP OpenView Client Configuration Manager ist eine Lösung zur Verwaltung von Hardware und Software für Windows XP- und HP Thin Client-Umgebungen, die bedienerfreundlich und schnell einsetzbar ist

und gleichzeitig eine solide Grundlage für zukünftige Anforderungen bietet. Für diese Lösung sind zwei Ausgaben erhältlich:

- Die Basic Edition ist ein kostenloses Produkt zur Verwaltung von HP Desktops, Notebooks und Workstations. Es enthält eine Hardware- und Software-Inventarfunktion, Fernbedienung, HP Alarmüberwachung, HP BIOS- und Treiber-Updates, Integration mit HP Protect Tools und zusätzlichen Support für Intel AMT. Die Basic Edition unterstützt außerdem den Einsatz und die Verwaltung von HP Thin Clients.
- Die im Handel erhältliche Premium Edition enthält alle Funktionen der Basic Edition und verfügt zusätzlich über Funktionen für Windows-Einsatz- und Migration, Patch-Verwaltung, Software-Verteilung und die Ermittlung der Software-Verwendung.

HP Client Configuration Manager bietet einen Migrationspfad zu HP OpenView PC Configuration Management Solution (basierend auf Radia-Technologie) für die automatisierte Verwaltung großer, heterogener und sich ständig verändernder IT-Umgebungen.

Weitere Informationen zu HP OpenView Client Configuration Manager finden Sie unter http://www.managementsoftware.hp.com/products/ccm/index.html.

HP OpenView PC Configuration Management Solution

HINWEIS: HP OpenView PC Configuration Manager Solution ist derzeit nicht für Windows Vista verfügbar.

HP OpenView PC Configuration Management Solution ist eine richtlinienbasierte Lösung, die es Administratoren ermöglicht, Software und Content auf heterogenen Client-Plattformen zu inventarisieren, einzusetzen und fortlaufend zu verwalten. Mit HP OpenView PC Configuration Management Solution haben IT-Experten folgende Möglichkeiten:

- Automatisierung des gesamten Lebenszyklusverwaltungsprozesses von der Erkennung über den Einsatz und die fortlaufende Verwaltung bis hin zu Migration und Außerbetriebnahme
- Automatischer Einsatz sowie fortlaufende Verwaltung und Aufrechterhaltung einer gesamten Software-Umgebung (Betriebssysteme, Anwendungen, Patches, Einstellungen und Inhalte) im gewünschten Zustand
- Software-Verwaltung auf praktisch jedem Gerät, einschließlich Desktops, Workstations und Notebooks, in einer heterogenen, eigenständigen Infrastruktur
- Software-Verwaltung auf den meisten Betriebssystemen

HP-Kunden berichten von erheblichen Einsparungen bei den IT-Kosten, kürzerer Time-to-Market für Software und Inhalte sowie einer deutlich höheren Produktivität und Zufriedenheit der Benutzer infolge des Einsatzes der ständigen Konfigurationsverwaltung.

Weitere Informationen zu HP OpenView PC Configuration Management Solution finden Sie unter http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Catalog for SMS

Die Verwaltung von Updates ist eine wichtige Funktion bei der Verwaltung von Computern, von Einzel-PCs bis hin zum Rechenzentrum eines Unternehmens. Die Fähigkeit, vorhandene Updates zu erkennen, und diese Updates dann rechtzeitig und automatisch durchzuführen, kann dazu beitragen, die Sicherheit und Produktivität für die verwaltete Organisation aufrecht zu erhalten. HP bietet jetzt einen Mechanismus zur effektiveren Durchführung von Updates für HP Systeme innerhalb einer Microsoft System Management Server Management-Infrastruktur. Der HP Client Catalog for SMS enthält Informationen zu Softwaretreibern und Patches für Desktop-, mobile und Workstation-Plattformen. Mit SMS 2003 R2 und Inventory Tool for Custom Updates können Organisationen HP Software-Updates schnell und einfach integrieren und einsetzen. Dies basiert auf detaillierten Plattformeigenschaften, die der HP Client Catalog for SMS enthält, um sich gezielt an entsprechende Client-Systeme innerhalb des verwalteten Unternehmens zu richten.

Weitere Informationen zu HP Client Catalog for SMS finden Sie unter http://www/hp/com/go/easydeploy/.

HP Backup and Recovery Manager

HP Backup and Recovery Manager ist eine benutzerfreundliche und vielseitige Anwendung, mit der Sie die primäre Festplatte des PCs sichern und wiederherstellen können. Die Anwendung arbeitet unter Windows und erstellt Sicherungskopien von Windows, allen Anwendungen und allen Datendateien. Sicherungen lassen sich so planen, dass sie automatisch in festgelegten Intervallen ausgeführt werden. sie können aber auch manuell gestartet werden. Wichtige Dateien können getrennt von gewöhnlichen Sicherungen archiviert werden.

HP Backup and Recovery Manager ist auf der Wiederherstellungspartition der Festplatte vorinstalliert und ermöglicht Ihnen Folgendes.

- Erstellen von Wiederherstellungspunkten, um das gesamte System inkrementell zu sichern.
- Sichern des gesamten Systems in einem einzigen Archiv.
- Sichern einzelner Dateien und Ordner.

Wiederherstellungspunkte und Dateisicherungen können auf CD oder DVD kopiert werden, und alle Sicherungen können in das Netzwerk oder auf sekundäre Festplatten kopiert werden.

HP empfiehlt dringend, sofort einen Wiederherstellungs-CD-Satz zu erstellen, bevor Sie den Computer benutzen, und regelmäßige automatische Wiederherstellungspunkt-Backups zu planen.

So erstellen Sie einen CD-Wiederherstellungssatz:

1. Klicken Sie auf **Start** > **HP Backup and Recovery** > **HP Backup** > **Recovery Manager**, um den Assistenten für Backup and Recovery zu öffnen. Klicken Sie dann auf **Weiter**.
2. Wählen Sie **Create a set of recovery discs (Recommended)** (Einen Wiederherstellungs-CD-Satz erstellen (empfohlen)), und klicken Sie dann auf **Weiter**.
3. Folgen Sie den Anleitungen des Assistenten.

Der HP Backup and Recovery Manager bietet zwei Wiederherstellungsmethoden. Die erste Methode – Wiederherstellung von Dateien und Ordnern – wird unter Windows ausgeführt. Für die zweite Methode – PC-Wiederherstellung – muss das System von der Wiederherstellungspartition oder vom Wiederherstellungs-CD-Satz gestartet werden. Drücken Sie beim Start die Funktionstaste F11, wenn die Meldung „Press F11 for Emergency Recovery“ (Drücken Sie F11 für Notfall-Wiederherstellung) angezeigt wird, um den Computer von der Wiederherstellungspartition zu booten.

Weitere Informationen zur Verwendung des HP Backup and Recovery Manager finden Sie im *HP Backup and Recovery Manager-Benutzerhandbuch* unter **Start** > **HP Backup and Recovery** > **HP Backup and Recovery Manager Manual**.

HINWEIS: Sie können im HP Support Center telefonisch einen Wiederherstellungs-CD-Satz bestellen. Rufen Sie die folgende Website auf, wählen Sie Ihre Region, und klicken Sie auf den Link **Technical support after you buy** (Kundenunterstützung nach dem Kauf) unter der Überschrift **Call HP** (HP anrufen), um die Telefonnummer des Support Centers für Ihre Region zu erfahren.

http://welcome.hp.com/country/us/en/wwcontact_us.html

Intel vPro-PCs mit Active Management Technology

Mit der Active Management Technology (AMT) von Intel lassen sich vernetzte Computerbestände optimal erfassen, pflegen und schützen. Dabei ermöglicht AMT die Verwaltung der PCs sowohl im eingeschalteten als auch im ausgeschalteten Zustand und sogar bei Betriebssystemabstürzen.

Intel vPro zeichnet sich durch folgende Vorteile aus:

- Bereitstellung von Hardware-Inventardaten
- Ausgabe von Warnmeldungen
- Power Management – Ein/Aus, Leistungswechsel
- Ferndiagnose und -reparatur
  - Seriell-über-LAN-Verbindung – Ermöglicht die Konsolensteuerung eines Remote-PCs während des Systemstarts
  - IDE-Redirect – Ermöglicht das Hochfahren des Systems unter Verwendung eines Remote-Bootlaufwerks, einer Remote-Festplatte oder eines ISO-Images
- Hardwarebasierte Isolierung und Wiederherstellung – Ermöglicht die Beschränkung bzw. Unterbindung des PC-Netzwerkzugriffs, falls eine verdächtige (Viren-)Aktivität entdeckt wird

HINWEIS: Weitere Informationen zur Intel vPro-Technologie finden Sie unter http://www.intel.com/vpro.

HP spezifische Informationen zur Intel vPro-Technologie finden Sie in den White Papers unter http://www.hp.com/support. Wählen Sie Ihr Land und Ihre Sprache aus. Wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen**, und geben Sie Ihre Modellnummer ein. Drücken Sie anschließend die Eingabetaste. Klicken Sie in der Kategorie **Ressourcen** auf **Handbücher** (Leitfäden, Zusatzinformationen, Ergänzungen usw.). Klicken Sie unter **Schnellaufruf von Handbüchern nach Kategorie...** auf **White Papers**.

Intel vPro-PCs verfügen über die folgenden Managementtechnologien:

- AMT
- ASF
- Virtualization Technology (VT)

ASF und AMT werden zwar beide unterstützt, dürfen jedoch nicht gleichzeitig konfiguriert sein.

So konfigurieren Sie Intel vPro-Systeme für AMT oder ASF:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Microsoft Windows auf **Start** > **Ausschalten** > **Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers die Tastenkombination Strg+P, sobald die Monitor-LED grün leuchtet.

   HINWEIS: Wenn Sie Strg+P nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut Strg+P drücken, sobald die Monitor-LED grün leuchtet.

Mit der oben angegebenen Tastenkombination rufen Sie das Intel Management Engine BIOS Execution (MEBx)-Setup-Dienstprogramm auf. Es ermöglicht Ihnen die Konfiguration diverser Aspekte der Managementtechnologie. Dabei stehen die folgenden Konfigurationsoptionen zur Verfügung:

- ME Platform Configuration
  - ME Platform State Control – Aktivierung/Deaktivierung der Management Engine
  - ME Firmware Local Update – Lokale Aktivierung/Deaktivierung der Verwaltung von Firmware-Updates
  - LAN Controller – Aktivierung/Deaktivierung des integrierten Netzwerk-Controllers
  - ME Features Control – Aktivierung von AMT, ASF oder keiner der beiden Funktionen
  - ME Power Control – Konfiguration der Stromsparrichtlinien für die Management Engine
- Intel AMT Configuration
  - Change AMT Password – Erforderlich zur Konfiguration von AMT (das Standardkennwort lautet **admin**)
  - Host Name – Ermöglicht dem Administrator die Zuweisung eines Client-Namens
  - TCP/IP – Ermöglicht dem Administrator die Zuweisung einer IP-Adresse bzw. die Aktivierung von DHCP
  - Provisioning Server – Ermöglicht dem Administrator die Zuweisung einer IP-Adresse zu dem bereitstellenden Server
  - Provision Model – Ermöglicht dem Administrator die Konfiguration des Unternehmens- oder SMB-Modus
  - Set PID and PPS – Ermöglicht dem Administrator die Bereitstellung des Pre-Provisioning-Schlüssels (siehe HP White Paper *Intel vPro Provisioning*)
  - Un-Provision – Ermöglicht dem Administrator die Rücksetzung der AMT-Konfiguration auf die Werkseinstellungen
  - VLAN – Ermöglicht dem Administrator die Aktivierung der LAN-Virtualisierungsunterstützung
  - SOL/IDE-R – Ermöglicht dem Administrator die Aktivierung von Remote-Boot- und -Steuersitzungen
- Change MEBx Password (HP empfiehlt dringend eine Änderung des MEBx-Kennworts vorzunehmen. Das Standardkennwort lautet **admin**.)

Zur Remote-Verwaltung von AMT-Systemen muss der Administrator eine Remote-Konsole verwenden, die AMT unterstützt. Unternehmensverwaltungskonsolen sind von Anbietern wie HP OpenView (derzeit nicht für Windows Vista verfügbar), Altiris und Microsoft SMS erhältlich. Im SMB-Modus stellt der Client eine Webbrowser-Oberfläche zur Verfügung. Um auf diese Funktion zuzugreifen, öffnen Sie einen Browser auf einem anderen System des Netzwerks und geben `http://host_name:16992` ein, wobei `host_name` der Name des betreffenden Systems ist. Alternativ können Sie anstelle des Host-Namens auch die IP-Adresse des Systems eingeben.

HP Proactive Change Notification

Proactive Change Notification (Benachrichtigung über Produktänderungen) versendet auf Basis der Eintragungen auf der sicheren Website Subscriber's Choice unaufgefordert automatisch folgende Mails:

- Eine PCN-E-Mail (Product Change Notification), in der Sie bis zu 60 Tage im Voraus über Änderungen an der Hard- und Software informiert werden. Dieser Service wird für die meisten Computer und Server bereitgestellt, die in Unternehmen eingesetzt werden.
- Eine E-Mail mit Informationen, Ratschlägen und Hinweisen für Kunden, Sicherheitsmitteilungen und Treiber-Warnmeldungen. Auch dieser Service gilt für die meisten, in Unternehmen genutzten Computer und Server.

Durch die Erstellung Ihres persönlichen Profils wird gewährleistet, dass Sie nur Informationen erhalten, die für Ihre konkrete IT-Umgebung relevant sind. Weitere Informationen zu PCN und zur Erstellung eines persönlichen Profils finden Sie unter http://h30046.www3.hp.com/subhub.php.

Subscriber’s Choice

Subscriber’s Choice ist ein Client-basierter HP Service.

Dabei stellt Ihnen HP ausgehend von Ihrem persönlichen Profil auf Sie abgestimmte Produkttipps, Artikel bzw. Treiber und Supportmeldungen/-benachrichtungen zur Verfügung.

In den von Subscriber’s Choice gesendeten E-Mails wird Ihnen mitgeteilt, dass die in Ihrem Profil angegebenen Informationen zum Abruf bereit stehen. Weitere Informationen zu Subscriber’s Choice und zur Erstellung eines persönlichen Profils finden Sie unter http://h30046.www3.hp.com/subhub.php.

Hinweis zur mitgelieferten Software

Bitte beachten Sie, dass die Softwarepakete Altiris Local Recovery und Dantz Retrospect nicht mehr im Lieferumfang von HP Business Desktops, Notebooks und Workstations enthalten sind. Ab 2006 werden sämtliche neuen Produkte dieser Kategorien mit HP Backup and Recovery Manager ausgeliefert.

5 ROM-Flash

Das BIOS Ihres Computers ist in einem programmierbaren Flash-ROM-Speicher (Read Only Memory, Nur-Lese-Speicher) gespeichert. Durch die Einrichtung eines Setup-Kennworts in Computer Setup (F10) Utility können Sie verhindern, dass der ROM-Speicher unbeabsichtigt aktualisiert oder überschrieben wird. Dies gewährleistet den fehlerfreien Betrieb des Computers. Falls Sie das BIOS aktualisieren möchten, können Sie von der HP Treiber- und Support-Website unter http://www.hp.com/support/files ein aktuelles BIOS-Image herunterladen.

ACHTUNG: Für den maximalen Schutz des ROM-Speichers müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert die unbefugte Aktualisierung des ROM-Speichers. Mithilfe von System Software Manager kann der Systemadministrator das Setup-Kennwort auf mehreren PCs gleichzeitig einstellen. Weitere Informationen finden Sie unter http://www.hp.com/go/ssm.

Remote ROM Flash

Remote ROM Flash ermöglicht dem Systemadministrator die sichere Aktualisierung des BIOS von entfernten HP Computern direkt über die zentrale Netzverwaltungskonsole. Indem der Systemadministrator diese Aufgabe auf mehreren Computern per Fernzugriff durchführen kann, lassen sich HP PC BIOS-Images über das Netzwerk konsistenter bereitstellen und besser überwachen. Dies führt außerdem zu höherer Produktivität und niedrigeren Total Cost of Ownership.

HINWEIS: SSM unterstützt derzeit keinen Remote-ROM-Flash auf Systemen mit aktiviertem Windows Vista BitLocker, die TPM-Maßnahmen zum Schutz der BitLocker-Schlüssel verwenden, da ein Flash des BIOS dazu führen würde, dass die von BitLocker für die Plattform erstellte Vertrauenssignatur ungültig wird. Aktivieren Sie BitLocker über die Gruppenrichtlinien, um ein Flash des System-BIOS herbeizuführen.

Der Computer muss eingeschaltet sein oder über die Remote Wakeup-Funktion eingeschaltet werden, wenn Remote ROM Flash verwendet wird.

Weitere Details zu Remote ROM Flash finden Sie in den Informationen zu HP Client Manager oder System Software Manager unter http://www.hp.com/go/ssm/.

HPQFlash

Das HPQFlash Dienstprogramm dient zur lokalen Aktualisierung oder Wiederherstellung des System-BIOS einzelner PCs unter Windows.

Weitere Informationen zu HPQFlash finden Sie unter http://www.hp.com/support/files. Geben Sie die Modellnummer des Computers ein, wenn Sie dazu aufgefordert werden.

6 Boot Block Emergency Recovery Mode

Der Boot Block Emergency Recovery Mode (Startblock-Wiederherstellungsmodus) ermöglicht eine Wiederherstellung des Systems im unwahrscheinlichen Falle eines ROM-Flash-Fehlers. Dieser Fall kann z. B. bei einem Stromausfall während eines BIOS-Upgrades auftreten, in dessen Folge der ROM-Flash unvollständig und das System-BIOS nicht nutzbar wäre. Der Startblock (Boot Block) ist ein flash-geschützter Bereich des ROM-Speichers und enthält Code, mit dem bei jedem Einschalten des Systems die Gültigkeit des BIOS-System-Images überprüft wird.

- Wenn das BIOS-Image des Systems gültig ist, startet das System normal.
- Wenn das BIOS-Image des Systems ungültig ist, bietet ein ausfallsicheres Boot-Block-BIOS ausreichend Unterstützung, um Wechseldatenträger für BIOS-Image-Dateien zu suchen. Wenn eine geeignete Datei gefunden wird, wird sie automatisch in den ROM-Speicher übernommen.

Wenn ein ungültiges BIOS-Image des Systems festgestellt wird, leuchtet die rote Betriebs-LED achtmal im Abstand von jeweils einer Sekunde. Gleichzeitig ertönt achtmal ein Warnton. Wenn der Teil des System-ROMs mit dem Image des Grafik-Options-ROM nicht beschädigt ist, erscheint die Meldung **Boot Block Emergency Recovery Mode** (Startblock-Wiederherstellungsmodus).

Wenn Sie das System wiederherstellen möchten, nachdem es in den Boot Block Emergency Recovery Mode umgeschaltet wurde, führen Sie die folgenden Schritte aus:

1. Schalten Sie den Computer aus.
2. Legen Sie eine CD ein bzw. schließen Sie ein USB-Flash-Gerät mit der gewünschten BIOS-Image-Datei im Hauptverzeichnis an.

   HINWEIS: Das verwendete Medium muss mit dem FAT12-, FAT16- oder FAT32-Dateisystem formatiert worden sein.
3. Schalten Sie den Computer ein.

   Wenn kein angemessenes BIOS-Image gefunden wird, werden Sie aufgefordert, ein Medium mit einer BIOS-Image-Datei einzulegen.

   Wenn der ROM-Speicher erfolgreich programmiert werden kann, wird das System automatisch heruntergefahren.
4. Entfernen Sie das Wechselmedium, mit dem das BIOS aktualisiert wurde.
5. Schalten Sie den Computer anschließend wieder ein, oder starten Sie ihn neu.

HINWEIS: BitLocker hindert Windows Vista am Starten, wenn sich eine CD mit der BIOS-Image-Datei in einem optischen Laufwerk befindet. Wenn BitLocker aktiviert ist, entnehmen Sie diese CD, bevor Sie versuchen, Windows Vista zu starten.

7 Replizieren des Setup

Mit dem folgenden Verfahren kann der Systemadministrator ohne großen Aufwand eine Setup-Konfiguration auf andere Computer des gleichen Modells kopieren. Dies ermöglicht eine schnellere und konsistentere Konfiguration mehrerer Computer.

HINWEIS: Bei diesem Verfahren benötigen Sie ein Diskettenlaufwerk oder ein unterstütztes USB-Flash-Media-Gerät wie einen HP Drive Key.

Kopieren auf einen einzigen Computer

ACHTUNG: Setup-Konfigurationen sind modellspezifisch. Wenn Ausgangs- und Zielcomputer nicht zum selben Modell gehören, kann das Dateisystem beschädigt werden. So darf beispielsweise keinesfalls die Setup-Konfiguration eines dc7xxx PC auf einen dx7xxx PC kopiert werden.

1. Wählen Sie die zu kopierende Setup-Konfiguration aus. Schalten Sie den Computer aus. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Herunterfahren**.
2. Wenn Sie ein USB-Flash-Media-Gerät verwenden, schließen Sie es jetzt an einen USB-Port des Computers an.
3. Schalten Sie den Computer ein.
4. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.
5. Wenn Sie eine Diskette verwenden, legen Sie sie jetzt ein.
6. Klicken Sie auf **Datei** > **Replicated Setup** (Setup-Replikation) > **Save to Removable Media** (Auf Wechsellaufwerk speichern). Folgen Sie den Bildschirmanleitungen, um die Konfigurationsdiskette oder das USB-Flash-Media-Gerät zu erstellen.
7. Schalten Sie den zu konfigurierenden Computer aus, und legen Sie die Konfigurationsdiskette ein, bzw. schließen Sie das USB-Flash-Media-Gerät an.
8. Schalten Sie den Computer anschließend wieder ein.
9. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.
10. Klicken Sie auf **Datei** > **Replicated Setup** (Setup-Replikation)> **Restore from Removable Media** (Von Wechsellaufwerk wiederherstellen), und folgen Sie den Anleitungen auf dem Bildschirm.
11. Starten Sie den Computer neu, sobald die Konfiguration abgeschlossen ist.

Kopieren auf mehrere Computer

△ **ACHTUNG:** Setup-Konfigurationen sind modellspezifisch. Wenn Ausgangs- und Zielcomputer nicht zum selben Modell gehören, kann das Dateisystem beschädigt werden. So darf beispielsweise keinesfalls die Setup-Konfiguration eines dc7xxx PC auf einen dx7xxx PC kopiert werden.

Bei diesem Verfahren dauert die Erstellung der Konfigurationsdiskette bzw. des USB-Flash-Media-Geräts etwas länger. Die Konfiguration auf die Zielcomputer nimmt dagegen sehr viel weniger Zeit in Anspruch.

HINWEIS: Bei diesem Verfahren benötigen Sie eine bootfähige Diskette oder ein bootfähiges USB-Flash-Media-Gerät. Wenn Sie nicht über Windows XP verfügen, um eine bootfähige Diskette zu erstellen, verwenden Sie das Verfahren für das Kopieren der Setup-Konfiguration auf einen einzelnen Computer (siehe „Kopieren auf einen einzigen Computer“ auf Seite 17).

1. Erstellen Sie eine bootfähige Diskette oder ein entsprechendes USB-Flash-Media-Gerät. Siehe „Unterstützte USB-Flash-Media-Geräte“ auf Seite 19 oder „Nicht unterstützte USB-Flash-Media-Geräte“ auf Seite 20.

   △ **ACHTUNG:** Nicht alle Computer lassen sich von einem USB-Flash-Media-Gerät starten. Wenn das USB-Gerät in der standardmäßigen Startreihenfolge im Dienstprogramm „Computer Setup (F10) Utility“ vor dem Festplattenlaufwerk aufgelistet ist, kann der Computer von einem USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

2. Wählen Sie die zu kopierende Setup-Konfiguration aus. Schalten Sie den Computer aus. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Herunterfahren**.
3. Wenn Sie ein USB-Flash-Media-Gerät verwenden, schließen Sie es jetzt an einen USB-Port des Computers an.
4. Schalten Sie den Computer ein.
5. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

6. Wenn Sie eine Diskette verwenden, legen Sie sie jetzt ein.
7. Klicken Sie auf **Datei** > **Replicated Setup** (Setup-Replikation) > **Save to Removable Media** (Auf Wechsellaufwerk speichern). Folgen Sie den Bildschirmanleitungen, um die Konfigurationsdiskette oder das USB-Flash-Media-Gerät zu erstellen.
8. Laden Sie ein BIOS-Dienstprogramm für das Replizieren der Setup-Konfiguration (repset.exe) herunter, und kopieren Sie es auf die Konfigurationsdiskette bzw. das USB-Flash-Media-Gerät. Um das Dienstprogramm zu erhalten, gehen Sie zu http://welcome.hp.com/country/us/en/support.html, und geben Sie die Modellnummer des betreffenden Computers ein.
9. Erzeugen Sie auf der Konfigurationsdiskette bzw. dem USB-Flash-Media-Gerät eine autoexec.bat-Datei mit dem folgenden Befehl:

   ```
   repset.exe
   ```

10. Schalten Sie den zu konfigurierenden Computer aus. Legen Sie die Konfigurationsdiskette ein, bzw. schließen Sie das USB-Flash-Media-Gerät an, und schalten Sie den Computer anschließend wieder ein. Das Konfigurationsdienstprogramm wird automatisch ausgeführt.
11. Starten Sie den Computer neu, sobald die Konfiguration abgeschlossen ist.

Erstellen eines bootfähiges Geräts

Unterstützte USB-Flash-Media-Geräte

Unterstützte Geräte verfügen über ein vorinstalliertes Image, mit dem sie sich schnell und einfach als bootfähige Geräte erstellen lassen. Alle HP oder Compaq sowie die meisten anderen USB-Flash-Media-Geräte sind mit diesem vorinstallierten Image ausgestattet. Wenn das betreffende Gerät nicht über ein derartiges Image verfügt, folgen Sie den Anleitungen weiter unten in diesem Abschnitt (siehe „Nicht unterstützte USB-Flash-Media-Geräte“ auf Seite 20).

Zum Erstellen einer bootfähigen Diskette oder eines entsprechenden USB-Flash-Media-Geräts wird Folgendes benötigt:

- ein unterstütztes USB-Flash-Media-Gerät
- eine bootfähige DOS-Diskette mit den Programmen FDISK und SYS (falls SYS nicht vorhanden ist, kann FORMAT verwendet werden; in diesem Fall gehen jedoch alle auf dem USB-Flash-Media-Gerät vorhandenen Dateien verloren)
- ein PC, der sich von einem USB-Flash-Media-Gerät starten lässt

△ **ACHTUNG:** Einige ältere PCs lassen sich unter Umständen nicht von einem USB-Flash-Media-Gerät starten. Wenn das USB-Gerät in der standardmäßigen Startreihenfolge im Dienstprogramm „Computer Setup (F10) Utility“ vor dem Festplattenlaufwerk aufgelistet ist, kann der Computer von einem USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

1. Schalten Sie den Computer aus.
2. Verbinden Sie das USB-Flash-Media-Gerät mit einem der USB-Ports des Computers, und entfernen Sie alle anderen USB-Speichergeräte mit Ausnahme der USB-Diskettenlaufwerke.
3. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und SYS.COM oder FORMAT.COM in ein Diskettenlaufwerk ein, und schalten Sie dann den Computer ein, um von der DOS-Diskette zu starten.
4. Starten Sie an der Eingabeaufforderung **A:** das Programm FDISK, indem Sie `FDISK` eingeben und danach die Eingabetaste drücken. Falls Sie dazu aufgefordert werden, klicken Sie auf **Yes** (**Y**), um die „Large Disk“-Unterstützung zu aktivieren.
5. Geben Sie den Wert `[5]` ein, um die Laufwerke des Systems anzeigen zu lassen. Das USB-Flash-Media-Gerät ist das Laufwerk, das am ehesten mit der Größe eines der aufgelisteten Laufwerke übereinstimmt. Meistens ist es das letzte Laufwerk in der Liste. Achten Sie dabei auf den Laufwerksbuchstaben.

   Laufwerk des USB-Flash-Media-Geräts: __________

   △ **ACHTUNG:** Wenn keines der angezeigten Laufwerke mit dem USB-Flash-Media-Gerät übereinstimmt, fahren Sie nicht fort, da es andernfalls zu Datenverlust kommen kann. Überprüfen Sie alle USB-Ports auf weitere Speichergeräte. Falls weitere Geräte vorhanden sein sollten, entfernen Sie sie, starten den Computer neu und fahren mit Schritt 4 fort. Wenn keine Geräte vorhanden sind, unterstützt das System entweder das betreffende USB-Flash-Media-Gerät nicht, oder das Gerät ist defekt. Versuchen Sie in diesem Fall NICHT weiter, das USB-Flash-Media-Gerät bootfähig zu machen.
6. Verlassen Sie FDISK durch Drücken der Esc-Taste, um zur Eingabeaufforderung **A:** zurückzukehren.
7. Wenn Ihre bootfähige DOS-Diskette SYS.COM enthält, fahren Sie mit Schritt 8 fort. Wenn dies nicht der Fall ist, fahren Sie mit Schritt 9 fort.
8. Geben Sie an der Eingabeaufforderung **A:** `SYS x:` ein, wobei x für den oben erwähnten Laufwerksbuchstaben steht.

△ **ACHTUNG:** Stellen Sie sicher, dass Sie den korrekten Laufwerksbuchstaben für das USB-Flash-Media-Gerät eingegeben haben.

Nach der Übertragung der Systemdateien kehrt SYS zur Eingabeaufforderung **A:** zurück. Fahren Sie mit Schritt 13 fort.

9. Kopieren Sie alle Dateien, die Sie behalten möchten, von Ihrem UBS-Flash-Media-Gerät in ein temporäres Verzeichnis auf einem anderen Laufwerk (z. B. auf dem internen Festplattenlaufwerk des Systems).

10. Geben Sie an der Eingabeaufforderung **A:** `FORMAT /S X:` ein, wobei `X` für den oben erwähnten Laufwerksbuchstaben steht.

△ **ACHTUNG:** Stellen Sie sicher, dass Sie den korrekten Laufwerksbuchstaben für das USB-Flash-Media-Gerät eingegeben haben.

FORMAT wird eine oder mehrere Warnmeldungen anzeigen und Sie jedes Mal fragen, ob Sie wirklich fortfahren möchten. Antworten Sie jedes Mal mit `Y` (Ja). FORMAT formatiert das USB-Flash-Media-Gerät, kopiert die Systemdateien und fordert Sie zur Eingabe einer Datenträgerkennung auf.

11. Falls Sie keine Kennung eingeben möchten, drücken Sie die Eingabetaste; andernfalls geben Sie die gewünschte Datenträgerkennung ein.

12. Kopieren Sie die in Schritt 9 gesicherten Dateien auf das USB-Flash-Media-Gerät.

13. Nehmen Sie die Diskette aus dem Laufwerk, und starten Sie den Computer neu. Der Computer startet von dem USB-Flash-Media-Gerät als Laufwerk C.

HINWEIS: Die standardmäßige Startreihenfolge variiert von Computer zu Computer und kann mit Computer Setup (F10) Utility geändert werden.

Wenn Sie eine DOS-Version unter Windows 9x verwendet haben, wird unter Umständen kurzfristig der Windows-Anmeldebildschirm angezeigt. Wenn dieser Bildschirm nicht erscheinen soll, fügen Sie dem Hauptverzeichnis des USB-Flash-Media-Geräts eine Datei mit Null-Länge und der Bezeichnung LOGO.SYS hinzu.

Kehren Sie zu „Kopieren auf mehrere Computer“ auf Seite 18 zurück.

Nicht unterstützte USB-Flash-Media-Geräte

Zum Erstellen einer bootfähigen Diskette oder eines entsprechenden USB-Flash-Media-Geräts wird Folgendes benötigt:

- ein USB-Flash-Media-Gerät
- eine bootfähige DOS-Diskette mit den Programmen FDISK und SYS (falls SYS nicht vorhanden ist, kann FORMAT verwendet werden; in diesem Fall gehen jedoch alle auf dem USB-Flash-Media-Gerät vorhandenen Dateien verloren)
- ein PC, der sich von einem USB-Flash-Media-Gerät starten lässt

△ **ACHTUNG:** Einige ältere PCs lassen sich unter Umständen nicht von einem USB-Flash-Media-Gerät starten. Wenn das USB-Gerät in der standardmäßigen Startreihenfolge im Dienstprogramm „Computer Setup (F10) Utility“ vor dem Festplattenlaufwerk aufgelistet ist, kann der Computer von einem USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

1. Wenn das System über PCI-Karten mit angeschlossenen SCSI-, ATA RAID- oder SATA-Laufwerken verfügt, schalten Sie den Computer aus und ziehen das Netzkabel.

△ **ACHTUNG:** Das Netzkabel muss UNBEDINGT gezogen werden.

2. Öffnen Sie die Gehäuseabdeckung, und entfernen Sie die PCI-Karten.

3. Verbinden Sie das USB-Flash-Media-Gerät mit einem der USB-Ports des Computers, und entfernen Sie alle anderen USB-Speichergeräte mit Ausnahme der USB-Diskettenlaufwerke. Bringen Sie die Gehäuseabdeckung wieder an.
4. Stecken Sie das Netzkabel ein, und schalten Sie den Computer ein.
5. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

6. Wechseln Sie zu **Erweitert** > **PCI Devices** (PCI-Geräte), um sowohl den PATA- als auch den SATA-Controller zu deaktivieren. Notieren Sie sich bei der Deaktivierung des SATA-Controllers dessen IRQ-Zuordnung, da Sie sie später wieder zuweisen müssen. Verlassen Sie das Setup-Programm, und bestätigen Sie dabei die vorgenommenen Änderungen.

   SATA-IRQ: __________

7. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und SYS.COM oder FORMAT.COM in ein Diskettenlaufwerk ein, und schalten Sie dann den Computer ein, um von der DOS-Diskette zu starten.
8. Führen Sie FDISK aus, und löschen Sie alle vorhandenen Partitionen auf dem USB-Flash-Media-Gerät. Erzeugen Sie eine neue Partition, und markieren Sie sie als die aktive Partition. Beenden Sie FDISK, indem Sie die Esc-Taste drücken.
9. Wenn das System beim Beenden von FDISK nicht automatisch neu gestartet wurde, drücken Sie Strg+Alt+Entf, um von der DOS-Diskette zu starten.
10. Geben Sie an der Eingabeaufforderung **A:** `FORMAT C: /S` ein, und drücken Sie dann die Eingabetaste. FORMAT formatiert das USB-Flash-Media-Gerät, kopiert die Systemdateien und fordert Sie zur Eingabe einer Datenträgerkennung auf.
11. Falls Sie keine Kennung eingeben möchten, drücken Sie die Eingabetaste; andernfalls geben Sie die gewünschte Datenträgerkennung ein.
12. Schalten Sie den Computer aus, und ziehen Sie das Netzkabel. Öffnen Sie die Gehäuseabdeckung, und setzen Sie die PCI-Karten wieder ein. Bringen Sie die Gehäuseabdeckung wieder an.
13. Stecken Sie das Netzkabel ein, nehmen Sie die Diskette aus dem Laufwerk, und schalten Sie dann den Computer wieder ein.
14. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.
15. Wechseln Sie zu **Erweitert** > **PCI Devices** (PCI-Geräte), und aktivieren Sie die PATA- und SATA-Controller, die in Schritt 6 deaktiviert wurden. Stellen Sie die ursprüngliche IRQ-Zuordnung für den SATA-Controller wieder her.
16. Speichern Sie die vorgenommenen Änderungen, und verlassen Sie das Programm. Der Computer startet von dem USB-Flash-Media-Gerät als Laufwerk C.

HINWEIS: Die standardmäßige Startreihenfolge variiert von Computer zu Computer und kann mit Computer Setup (F10) Utility geändert werden. Anleitungen hierzu finden Sie im *Computer Setup (F10) Utility Guide* auf der *Documentation and Diagnostics CD*.

Wenn Sie eine DOS-Version unter Windows 9x verwendet haben, wird unter Umständen kurzfristig der Windows-Anmeldebildschirm angezeigt. Wenn dieser Bildschirm nicht erscheinen soll, fügen Sie dem Hauptverzeichnis des USB-Flash-Media-Geräts eine Datei mit Null-Länge und der Bezeichnung LOGO.SYS hinzu.

Kehren Sie zu „Kopieren auf mehrere Computer“ auf Seite 18 zurück.

8 Dual-State-Netzschalter

Bei aktivierter ACPI-Funktion (Advanced Configuration and Power Interface) übernimmt der Netzschalter entweder die Funktion des Ein-/Aus-Schalters oder der Standby-Taste. In der Funktion als Standby-Taste unterbricht er die Stromzufuhr nicht, sondern schaltet den Computer auf einen geringen Stromverbrauch um. Dadurch können Sie schnell in den Energiesparmodus schalten, ohne die Anwendungen schließen zu müssen; außerdem können Sie ohne Datenverlust schnell in den vorherigen Betriebszustand zurückkehren.

So ändern Sie die Konfiguration des Netzschalters:

1. Klicken Sie mit der linken Maustaste auf **Start**, **Systemsteuerung** > **Energieoptionen**.
2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Erweitert**.
3. Wählen Sie im Abschnitt **Netzschaltervorgänge** die Option **In den Standby-Modus wechseln** aus.

Nachdem Sie den Netzschalter als Standby-Taste konfiguriert haben, können Sie das System mit dem Schalter auf einen sehr geringen Stromverbrauch (Standby-Modus) umschalten. Durch erneutes Drücken der Standby-Taste schalten Sie aus dem Standby-Modus auf Normalbetrieb um. Wenn Sie die Stromzufuhr ganz unterbrechen wollen, halten Sie den Netzschalter vier Sekunden lang gedrückt.

△ **ACHTUNG:** Schalten Sie den Computer nur über den Netzschalter aus, wenn das System nicht mehr reagiert. Fahren Sie den Computer ansonsten über die Optionen des Betriebssystems herunter, da ansonsten die Gefahr der Beschädigung oder des Verlusts von Daten auf der Festplatte besteht.

9 HP Website-Support

Die HP Techniker testen die von HP und Drittanbietern entwickelte Software nach strengen Kriterien und entwickeln auf das jeweilige Betriebssystem zugeschnittene Support-Software, um so eine optimale Leistung, Kompatibilität und Zuverlässigkeit von HP Computern zu gewährleisten.

Wenn Sie ein neues oder überarbeitetes Betriebssystem auf Ihrem Computer installieren, sollten Sie unbedingt auch die für das jeweilige Betriebssystem entwickelte Support-Software installieren. Wenn Sie mit einer anderen als der vorinstallierten Version von Microsoft Windows arbeiten möchten, müssen Sie die entsprechenden Gerätetreiber und Dienstprogramme installieren. Nur so ist sichergestellt, dass alle Funktionen unterstützt werden und einwandfrei arbeiten.

HP hat das Auffinden, den Zugriff, die Bewertung und die Installation der neuesten Support-Software erheblich vereinfacht. Sie können die Software unter folgender Adresse herunterladen: http://www.hp.com/support.

Die Website enthält die neuesten Gerätetreiber, Dienstprogramme und Flash-ROM-Images, die zur Ausführung des aktuellen Microsoft Windows Betriebssystems auf Ihrem HP Computer erforderlich sind.

10 Branchenstandards

HP Management Lösungen können in andere Systemverwaltungslösungen integriert werden. Unter anderem werden die folgenden Branchenstandards beachtet:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake-on-LAN-Technologie
- ACPI
- SMBIOS
- PXE (Pre-boot Execution)-Unterstützung

11 Bestandsüberwachung und Sicherheit

Die auf dem Computer vorinstallierten Funktionen zur Bestandsüberwachung stellen Ihnen wichtige Informationen bereit, die über HP Systems Insight Manager, HP Client Manager, HP OpenView PC Configuration Management, OpenView Client Configuration Manager und Asset Management Solutions (derzeit nicht für Windows Vista verfügbar) sowie andere Management-Anwendungen verwaltet werden können. Durch die nahtlose und automatische Integration in diese Produkte können Sie das Management-Tool auswählen, das für Ihre Umgebung am besten geeignet ist, ohne Ihre vorhandenen Investitionen in entsprechende Tools zu gefährden.

Darüber hinaus bietet HP mehrere Lösungen zur Steuerung des Zugriffs auf wichtige Komponenten und Daten an. HP Embedded Security for ProtectTools unterbindet – sofern es installiert wurde – den unbefugten Zugriff auf Daten, überprüft die Systemintegrität und authentifiziert Fremdnutzer, die auf das System zugreifen möchten. (Weitere Informationen finden Sie unter *HP ProtectTools Security Manager Guide* auf http://www.hp.com.) Sicherheitsfunktionen wie HP Embedded Security for ProtectTools, Smart Cover Sensor und Smart Cover Lock, die in einigen Modellen verfügbar sind, helfen, unautorisierten Zugriff auf interne Bestandteile des PCs zu verhindern. Durch die Deaktivierung von parallelen und seriellen Anschlüssen sowie USB-Ports oder durch die Deaktivierung der Bootfähigkeit von Wechsellaufwerken können Sie wertvolle Datenbestände schützen. Memory Change- und Smart Cover Sensor-Warnmeldungen können automatisch an die jeweiligen Systemverwaltungsprogramme weitergeleitet werden, um darauf aufmerksam zu machen, dass sich eine unbefugte Person Zugang zu den internen Computerkomponenten verschaffen möchte.

HINWEIS: HP Embedded Security for ProtectTools, der Smart Cover Sensor und das Smart Cover Lock sind optionale Merkmale, die nur für bestimmte Modelle zur Verfügung stehen.

Verwenden Sie die folgenden Dienstprogramme zur Verwaltung der Sicherheitseinstellungen auf HP Computern:

- Lokal, mit Hilfe von Computer Setup Utility. Weitere Informationen und Anleitungen zur Verwendung der Computer Setup-Dienstprogramme finden Sie in dem im Lieferumfang enthaltenen *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*. Einige Computer verfügen darüber hinaus über HP BIOS Configuration for ProtectTools, eine Windows-basierte ProtectTools Komponente, mit der Administratoren BIOS-Sicherheitseinstellungen bei laufendem Betriebssystem konfigurieren können.
- Remote, mit HP Client Manager Software, OpenView Client Configuration Manager oder System Software Manager. Diese Software ermöglicht den sicheren, einheitlichen Einsatz und die Steuerung von Sicherheitseinstellungen.

Die folgende Tabelle und die zugehörigen Abschnitte beziehen sich auf die lokale Verwaltung von Sicherheitsfunktionen über Computer Setup Utility (F10).

Tabelle 11-1 Sicherheitsfunktionen – Übersicht

Option	Beschreibung
Setup Password (Setup-Kennwort)	Ermöglicht das Einrichten und Aktivieren des Setup-Kennworts (Administrator-Kennwort).

Tabelle 11-1 Sicherheitsfunktionen – Übersicht (Fortsetzung)

Option	Beschreibung
	HINWEIS: Wenn ein Setup-Kennwort eingerichtet wurde, ist seine Eingabe erforderlich, um die Optionen für Computer Setup zu ändern, den ROM-Speicher zu aktualisieren oder Änderungen an bestimmten Plug-and-Play-Einstellungen unter Windows vorzunehmen. Weitere Informationen finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.
Power-On Password (Kennwort für den Systemstart)	Ermöglicht das Einrichten und Aktivieren des Kennworts für den Systemstart. Weitere Informationen finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.
Password Options (Kennwortoptionen) (Diese Auswahl wird nur dann angezeigt, wenn ein Benutzerkennwort eingerichtet wurde.)	Hiermit können Sie festlegen, ob für ein Kennwort für den Warmstart (Strg+Alt+Entf) erforderlich ist. Weitere Informationen finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.
Pre-Boot Authorization (Autorisierung vor dem Bootvorgang)	Ermöglicht die Aktivierung bzw. Deaktivierung der Smart Card, die anstelle des Kennworts für den Systemstart verwendet werden kann.
Smart Cover	Ermöglicht die folgenden Einstellungen: • Aktivieren und Deaktivieren des Smart Cover Lock • Aktivieren und Deaktivieren des Cover Removal Sensor **HINWEIS:** Mit *Notify User* (Benutzer benachrichtigen) wird der Benutzer benachrichtigt, falls der Sensor erkennt, dass die Abdeckung entfernt wurde. Mit *Setup Password* (Setup-Kennwort) wird festgelegt, dass das Setup-Kennwort zum Starten des Computers eingegeben werden muss, falls der Sensor erkannt hat, dass die Abdeckung entfernt wurde. Diese Funktion wird nur von bestimmten Modellen unterstützt. Weitere Informationen finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.
Embedded Security (Embedded Security-Chip)	Ermöglicht die folgenden Einstellungen: • Aktivieren und Deaktivieren des Embedded Security-Chips • Zurücksetzen des Chips auf die Werkseinstellungen Diese Funktion wird nur bei bestimmten Modellen unterstützt. Weitere Informationen finden Sie im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com.
Device Security (Gerätesicherheit)	Aktiviert bzw. deaktiviert die seriellen Anschlüsse, den parallelen Anschluss, die USB-Ports an der Computervorderseite, das Audiosystem, die Netzwerk-Controller (nur bestimmte Modelle) sowie die SCSI-Controller (nur bestimmte Modelle).
Network Service Boot (Starten über Netzwerk)	Ermöglicht das Aktivieren bzw. Deaktivieren der Funktion, mit der der Computer mit einem Betriebssystem gestartet werden kann, das auf einem Netzwerkserver installiert ist. (Der Netzwerk-Controller muss sich auf dem PCI-Bus befinden oder auf der Systemplatine integriert sein.)
System IDs (System-IDs)	Ermöglicht die folgenden Einstellungen: • Bestandskennung (18-Byte-Kennung) und Eigentümerkennung (80-Byte-Kennung, die während des POST angezeigt wird). Weitere Informationen finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*. • Seriennummer auf dem Gehäuse oder UUID-Nummer (Universal Unique Identifier). Die UUID kann nur geändert werden, wenn die aktuelle Seriennummer des Gehäuses ungültig ist. (Diese Nummern

Tabelle 11-1 **Sicherheitsfunktionen – Übersicht (Fortsetzung)**

Option	Beschreibung
	werden in der Regel im Werk vergeben und zur eindeutigen Identifizierung des Systems verwendet.) Landesspezifische Tastatureinstellungen (z. B. Englisch oder Deutsch) für die Eingabe der System-ID.
DriveLock (nur bestimmte Modelle)	Ermöglicht die Zuweisung oder Änderung eines Master- oder Benutzerkennworts für ATA-Festplatten. Bei Aktivierung dieser Funktion wird der Benutzer dazu aufgefordert, während des POST eines der DriveLock-Kennwörter einzugeben. Wird kein Kennwort erfolgreich eingegeben, kann so lange nicht auf die Festplatte zugegriffen werden, bis bei nachfolgenden Kaltstarts eines der Kennwörter erfolgreich eingegeben wird. **HINWEIS:** Diese Option wird nur angezeigt, wenn mindestens ein an das System angeschlossenes ATA-Laufwerk den ATA-Befehlssatz für die Systemsicherheit unterstützt. Weitere Informationen finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.

Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.

Je nach Computerkonfiguration werden unterschiedliche Sicherheitsfunktionen unterstützt.

Kennwortschutz

Das Kennwort für den Systemstart verhindert eine unbefugte Verwendung des Computers, indem für den Zugriff auf Anwendungen oder Daten bei jedem Einschalten oder Neustart des Computers die Eingabe eines Kennworts verlangt wird. Das Setup-Kennwort verhindert insbesondere den unbefugten Zugriff auf Computer Setup und kann auch zur Übergehung des Kennworts für den Systemstart verwendet werden. Dabei wird auch dann der Zugriff auf den Computer gewährt, wenn bei der Eingabeaufforderung für das Systemstart-Kennwort statt dessen das Setup-Kennwort eingegeben wird.

Dabei kann ein Kennwort für das gesamte Netzwerk festgelegt werden, so dass der Systemadministrator sich für Wartungsarbeiten bei allen Netzwerksystemen anmelden kann, ohne das betreffende Kennwort für den Systemstart zu kennen.

Einrichten eines Setup-Kennworts über Computer Setup

Weitere Informationen zu Systemen mit einem Embedded Security-Chip finden Sie im *HP ProtectTools Security Manager-Handbuch* auf http://www.hp.com. Wenn ein Setup-Kennwort über Computer Setup eingerichtet wird, können Sie den Computer nur dann über Computer Setup Utility (F10) neu konfigurieren, wenn Sie das Kennwort eingeben.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Setup Password** (Setup-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Bevor Sie das Menü verlassen, klicken Sie auf **File** (Datei) > **Save Changes and Exit** (Änderungen speichern und schließen).

Einrichten eines Kennworts beim Systemstart über Computer Setup

Die Einrichtung eines Kennworts für den Systemstart über Computer Setup verhindert den unbefugten Zugriff auf den Computer, wenn kein Kennwort eingegeben wird. Wenn ein Kennwort für den Systemstart festgelegt wurde, zeigt Computer Setup im Sicherheitsmenü eine Reihe von Kennwortoptionen an. Als Kennwortoptionen steht u. a. **Password Prompt on Warm Boot** (Aufforderung zur Eingabe des Kennworts beim Warmstart) zur Auswahl. Bei Aktivierung dieser Option muss das Kennwort auch bei jedem Neustart eingegeben werden.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.

2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Power-On Password** (Systemstart-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.

4. Bevor Sie das Menü verlassen, klicken Sie auf **File** (Datei) > **Save Changes and Exit** (Änderungen speichern und schließen).

Eingeben eines Kennworts für den Systemstart

Führen Sie die folgenden Schritte durch, um ein Kennwort für den Systemstart einzugeben:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Ausschalten** > **Neu starten**.

2. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das aktuelle Kennwort ein und drücken dann die Eingabetaste.

   HINWEIS: Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

Eingeben eines Setup-Kennworts

Weitere Informationen zu Systemen mit einem Embedded Security-Chip finden Sie im *HP ProtectTools Security Manager-Handbuch* auf http://www.hp.com.

Wenn für den Computer ein Setup-Kennwort eingerichtet wurde, werden Sie jedes Mal zur Eingabe dieses Kennworts aufgefordert, wenn Sie das Programm Computer Setup starten.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.

2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das Setup-Kennwort ein, und drücken Sie die Eingabetaste.

HINWEIS: Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

Ändern des Kennworts für den Systemstart oder des Setup-Kennworts

Weitere Informationen zu Systemen mit einem Embedded Security-Chip finden Sie im *HP ProtectTools Security Manager-Handbuch* auf http://www.hp.com.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Ausschalten** > **Neu starten**.

2. Zum Ändern des Systemstart-Kennworts fahren Sie mit Schritt 3 fort.

   Um das Setup-Kennwort zu ändern, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort, einen Schrägstrich (/) oder ein anderes Begrenzungszeichen, das neue Kennwort, einen weiteren Schrägstrich(/) bzw. ein anderes Begrenzungszeichen und ein zweites Mal das neue Kennwort ein, so dass der Eintrag wie folgt aussieht: `aktuelles Kennwort/neues Kennwort/neues Kennwort`

   HINWEIS: Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

4. Drücken Sie die Eingabetaste.

Das neue Kennwort gilt ab dem nächsten Start des Computers.

HINWEIS: Weitere Informationen zu Begrenzungszeichen finden Sie unter „Begrenzungszeichen auf landesspezifischen Tastaturen“ auf Seite 31. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in Computer Setup geändert werden.

Löschen des Kennworts für den Systemstart oder des Setup-Kennworts

Weitere Informationen zu Systemen mit einem Embedded Security-Chip finden Sie im *HP ProtectTools Security Manager-Handbuch* auf http://www.hp.com.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Ausschalten** > **Neu starten**.

2. Zum Löschen des Systemstart-Kennworts fahren Sie mit Schritt 3 fort.

   Um das Setup-Kennwort zu löschen, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort und einen Schrägstrich (/) oder ein anderes Begrenzungszeichen ein (siehe unten): `aktuelles Kennwort/`

4. Drücken Sie die Eingabetaste.

HINWEIS: Weitere Informationen zu Begrenzungszeichen finden Sie unter „Begrenzungszeichen auf landesspezifischen Tastaturen“ auf Seite 31. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in Computer Setup geändert werden.

Begrenzungszeichen auf landesspezifischen Tastaturen

Jede Tastatur wurde an die landesspezifischen sprachlichen Besonderheiten angepasst. Die Syntax und die Tasten, die Sie zum Ändern oder Löschen des Kennworts verwenden, sind abhängig von der Anordnung der Tasten auf Ihrer Tastatur.

Begrenzungszeichen auf landesspezifischen Tastaturen					
/	Arabisch	-	Griechisch	/	Russisch
=	Belgisch	.	Hebräisch	-	Slowakisch
-	BHKSJ*	-	Ungarisch	-	Spanisch
/	Brasilianisch	-	Italienisch	/	Schwedisch/Finnisch
/	Chinesisch	/	Japanisch	-	Schweizerisch
-	Tschechisch	/	Koreanisch	/	Taiwanesisch
-	Dänisch	-	Lateinamerikanisch (Spanisch/ Portugiesisch)	/	Thailändisch
!	Französisch	-	Norwegisch	.	Türkisch
é	Kan. Französisch	-	Polnisch	/	Amerikanisches Englisch
-	Deutsch	-	Portugiesisch		
	* Bosnien-Herzegowina, Kroatien, Slowenien und Jugoslawien				

Löschen von Kennwörtern

Wenn Sie Ihr Benutzerkennwort vergessen haben, können Sie nicht mehr auf Ihren Computer zugreifen. Anleitungen zum Löschen von Kennwörtern finden Sie im *Fehlerbeseitigungs-Handbuch* auf der *Documentation and Diagnostics CD*.

Weitere Informationen zu Systemen mit einem Embedded Security-Chip finden Sie im *HP ProtectTools Security Manager-Handbuch* auf http://www.hp.com.

DriveLock

DriveLock ist eine Sicherheitsfunktion nach Branchenstandard, die den unbefugten Zugriff auf die Daten von ATA-Festplatten verhindert. DriveLock wurde als Erweiterung von Computer Setup entwickelt. Die Funktion steht nur für Laufwerke zur Verfügung, die den ATA-Befehlssatz für die Systemsicherheit unterstützen. DriveLock richtet sich an HP Kunden, deren oberste Priorität der Schutz der Daten ist. Für diese Kunden stehen die Kosten einer Festplatte und der Verlust der darauf gespeicherten Daten in keinem Verhältnis zu dem Schaden, der durch den unberechtigten Zugriff auf ihren Inhalt entstehen kann. Damit dieses hohe Sicherheitsniveau im Falle eines vergessenen Kennworts keine allzu großen

Probleme verursacht, verwendet die HP Implementierung von DriveLock ein Sicherheitssystem mit zwei Kennwörtern. Dabei sollte ein Kennwort vom Systemadministrator festgelegt und verwendet werden, während das zweite normalerweise vom Benutzer erstellt und verwendet wird. Wenn beide Kennwörter vergessen werden, gibt es keine Möglichkeit mehr, die Laufwerksperre aufzuheben. Deshalb ist die Verwendung von DriveLock am sichersten, wenn die auf der Festplatte enthaltenen Daten in ein Firmeninformationssystem repliziert oder regelmäßig gesichert werden. Für den Fall, dass beide DriveLock-Kennwörter vergessen werden, bleibt der Zugriff auf die Festplatte für immer gesperrt. Dies stellt für Benutzer, die nicht dem obigen Kundenprofil entsprechen, unter Umständen ein inakzeptables Risiko dar. Für Benutzer, die diesem Profil entsprechen, ist dieses Risiko angesichts der auf der Festplatte gespeicherten Daten jedoch absolut akzeptabel.

Verwenden von DriveLock

Wenn eines oder mehrere Laufwerke den ATA-Befehlssatz für die Systemsicherheit unterstützen, wird im Sicherheitsmenü von Computer Setup die DriveLock-Option angezeigt. Der Benutzer kann wählen, ob er das Master-Kennwort festlegen oder DriveLock aktivieren möchte. Zur Aktivierung von DriveLock muss ein Benutzerkennwort eingegeben werden. Da die erste Konfiguration von DriveLock normalerweise vom Systemadministrator ausgeführt wird, sollte zuerst ein Masterkennwort festgelegt werden. HP empfiehlt die Festlegung eines Masterkennworts durch den Administrator, unabhängig davon, ob DriveLock aktiviert werden soll oder nicht. Dadurch hat der Administrator die Möglichkeit, DriveLock-Einstellungen zu ändern, wenn das Laufwerk einmal gesperrt sein sollte. Nachdem das Masterkennwort festgelegt wurde, kann der Administrator DriveLock aktivieren oder es deaktiviert lassen.

Im Fall einer gesperrten Festplatte fragt POST ein Kennwort zur Entsperrung ab. Wenn ein Kennwort für den Systemstart festgelegt wurde, das dem Benutzerkennwort des Geräts entspricht, fordert POST den Benutzer nicht zur erneuten Eingabe des Kennworts auf. Andernfalls wird der Benutzer zur Eingabe eines DriveLock-Kennworts aufgefordert. Bei einem Kaltstart kann entweder das Master- oder das Benutzerkennwort verwendet werden. Bei einem Warmstart muss dasselbe Kennwort eingegeben werden, mit dem das Laufwerk beim vorhergegangenen Kaltstart entsperrt wurde. Dabei haben die Benutzer zwei Versuche zur Kennworteingabe. Wenn bei einem Kaltstart zweimal das falsche Kennwort eingegeben wurde, wird POST zwar fortgesetzt, es besteht aber weiterhin kein Zugriff auf die Festplatte. Wenn der Benutzer bei einem Warmstart oder einem Neustart von Windows zweimal das falsche Kennwort eingegeben hat, wird POST angehalten, und der Benutzer wird aufgefordert, das System aus- und wieder einzuschalten.

Anwendungen von DriveLock

Den größten Nutzen entfaltet die DriveLock-Sicherheitsfunktion in einer Unternehmensumgebung. Dort hat der Systemadministrator die Aufgabe, die Festplatte zu konfigurieren und damit u. a. auch das DriveLock-Masterkennwort sowie ein temporäres Benutzerkennwort einzurichten. Falls ein Benutzer das Benutzerkennwort vergisst oder das Gerät an einen anderen Mitarbeiter weitergegeben wird, kann das Masterkennwort dazu verwendet werden, das Benutzerkennwort zurückzusetzen oder auf die Festplatte zuzugreifen.

HP empfiehlt Systemadministratoren, die DriveLock aktivieren möchten, die Erstellung einer Firmenrichtlinie zur Einrichtung und Verwaltung von Masterkennwörtern. Dadurch soll vermieden werden, dass ein Mitarbeiter vor seinem Ausscheiden aus der Firma absichtlich oder unabsichtlich beide DriveLock-Kennwörter festlegt. In einem solchen Fall würde die Festplatte unbrauchbar und müsste ersetzt werden. Außerdem könnte es passieren, dass Systemadministratoren, die kein Masterkennwort festlegen, selbst eine gesperrte Festplatte vorfinden und dadurch keine Routineüberprüfungen auf nicht autorisierte Software, andere Bestandskontrollfunktionen und Supportaktivitäten mehr ausführen können.

Benutzern mit niedrigeren Sicherheitsanforderungen empfiehlt HP die Aktivierung von DriveLock nicht. Dazu zählen private Benutzer oder Benutzer, die auf ihrer Festplatte im Normalfall keine streng geheimen Daten aufbewahren. Für diese Benutzer ist der mögliche Verlust einer Festplatte aufgrund von zwei vergessenen Kennwörtern größer als der Wert, der mit DriveLock geschützt werden soll. Der Zugriff auf Computer Setup und DriveLock kann durch das Setup-Kennwort eingeschränkt werden.

Durch das Festlegen eines Setup-Kennworts, das nicht an Endbenutzer weitergegeben wird, können Systemadministratoren vermeiden, dass Benutzer DriveLock aktivieren.

Smart Cover Sensor

Der CoverRemoval Sensor (nur bei bestimmten Modellen) ist eine Kombination aus Hardware- und Softwaretechnologie. Er gibt eine Warnmeldung aus, wenn die Gehäuseabdeckung oder die Seitenabdeckungen entfernt wurden. Es gibt drei Schutzstufen, die in der folgenden Tabelle beschrieben werden.

Tabelle 11-2 Smart Cover Sensor – Schutzstufen

Stufe	Einstellung	Beschreibung
Stufe 0	Disabled (Deaktiviert)	Der Smart Cover Sensor ist deaktiviert (Standardeinstellung).
Stufe 1	Notify User (Benutzer benachrichtigen)	Wenn der Computer neu gestartet wird, wird gemeldet, dass die Gehäuseabdeckung bzw. die Seitenabdeckungen entfernt wurden.
Stufe 2	Setup Password (Setup-Kennwort)	Wenn der Computer neu gestartet wird, wird gemeldet, dass die Gehäuseabdeckung bzw. die Seitenabdeckungen entfernt wurden. Sie müssen das Setup-Kennwort eingeben, um fortfahren zu können.

HINWEIS: Diese Einstellungen können mit Hilfe von Computer Setup geändert werden. Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility-Handbuch* auf der *Documentation and Diagnostics CD*.

Einstellen der Schutzstufe für den Smart Cover Sensor

So legen Sie die Schutzstufe für den Smart Cover Sensor fest:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.
3. Wählen Sie **Security** (Sicherheit) > **Smart Cover** > **Cover Removal Sensor**, und aktivieren Sie dann die gewünschte Schutzstufe.
4. Bevor Sie das Menü verlassen, klicken Sie auf **File** (Datei) > **Save Changes and Exit** (Änderungen speichern und schließen).

Smart Cover Lock

Das Smart Cover Lock ist eine softwaregesteuerte Gehäusesperre, mit der eine Reihe von HP Computern ausgestattet sind. Sie verhindert den unbefugten Zugriff auf die internen Komponenten des Computers. Die Computer werden mit deaktiviertem Smart Cover Lock geliefert.

ACHTUNG: Für eine maximale Sicherheit der Gehäusesperre müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert den unbefugten Zugriff auf Computer Setup.

HINWEIS: Das Smart Cover Lock ist als Zusatzoption für bestimmte Systeme erhältlich.

Sperren des Smart Cover Lock

So aktivieren (sperren) Sie das Smart Cover Lock:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wählen Sie **Security** (Sicherheit) > **Smart Cover** > **Cover Lock** (Gehäusesperre) > **Lock option** (Sperroption).
4. Bevor Sie das Menü verlassen, klicken Sie auf **File** (Datei) > **Save Changes and Exit** (Änderungen speichern und schließen).

Aufheben der Sperre des Smart Cover Lock

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, sobald die Monitor-LED grün leuchtet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut F10 drücken, sobald die Monitor-LED grün leuchtet.

3. Wählen Sie **Security** (Sicherheit) > **Smart Cover** > **Cover Lock** (Gehäusesperre) > **Unlock** (Entsperren).
4. Bevor Sie das Menü verlassen, klicken Sie auf **File** (Datei) > **Save Changes and Exit** (Änderungen speichern und schließen).

Verwenden des Smart Cover FailSafe-Schlüssels

Wenn das Smart Cover Lock aktiviert ist und Sie das Benutzerkennwort nicht eingeben können, um die Sperre zu deaktivieren, brauchen Sie einen Smart Cover FailSafe-Schlüssel, um die Gehäuseabdeckung öffnen zu können. Sie brauchen den Schlüssel in den folgenden Fällen:

- Stromausfall
- Fehlgeschlagener Systemstart
- Ausfall einer PC-Komponente (z. B. Prozessor oder Netzteil)
- Vergessenes Kennwort

ACHTUNG: Der Smart Cover FailSafe-Schlüssel ist ein spezielles Tool, das von HP angeboten wird. Sie sollten es von einem HP Servicepartner bestellen, bevor der Ernstfall tatsächlich eintritt.

Führen Sie eines der folgenden Verfahren durch, um den FailSafe-Schlüssel zu erhalten:

- Wenden Sie sich an einen HP Servicepartner.
- Rufen Sie die in der Garantieerklärung genannte Rufnummer an.

Weitere Informationen zur Verwendung des Smart Cover FailSafe-Schlüssels finden Sie im *Hardware-Referenzhandbuch* auf der *Documentation and Diagnostics CD*.

Kabel-Diebstahlsicherung

Sie können an der Anschlussleiste auf der Rückseite des Computers eine Kabel-Diebstahlsicherung anbringen und damit den Computer an einen fest installierten Gegenstand anschließen.

Anleitungen mit den entsprechenden Abbildungen finden Sie im *Hardware-Referenzhandbuch* auf der *Documentation and Diagnostics CD*.

Fingerprint Identification Technology

Die HP Fingerprint Identification Technology macht die Eingabe eines Benutzerkennworts überflüssig, erhöht die Netzwerksicherheit, vereinfacht den Anmeldungsvorgang und verringert die mit dem Management von Firmennetzwerken verbundenen Kosten. Wegen ihres erschwinglichen Preises ist sie nicht mehr nur High-Tech-Organisationen mit hohem Sicherheitsbedürfnis vorbehalten.

HINWEIS: Die Unterstützung für die Fingerprint Identification Technology hängt von dem jeweiligen Modell ab.

Weitere Informationen finden Sie unter folgender Adresse:

http://h18004.www1.hp.com/products/security/.

Fehlermeldung und -beseitigung

Durch die Kombination von innovativer Hardware- und Softwaretechnologie sorgen die Funktionen zur Fehlermeldung und Fehlerbehebung dafür, dass der Datenverlust und Ausfallzeiten vermieden werden.

Wenn der Computer an ein Netzwerk angeschlossen ist, das von HP Client Manager überwacht wird, sendet er eine Fehlermeldung an die Netzwerk-Management-Anwendung. HP Client Manager Software ermöglicht aber auch die Remote-Einplanung von Diagnosetests, so dass diese automatisch auf allen verwalteten PCs ausgeführt und eventuell festgestellte Fehler in einem Bericht protokolliert werden.

Drive Protection System

Das Drive Protection System (DPS) ist ein Diagnose-Tool, mit dem die Festplatten bestimmter HP Computer ab Werk ausgestattet sind. Das Programm soll die Diagnose von Problemen ermöglichen, die andernfalls zu einem unnötigen Festplattenaustausch führen könnten.

Jede Festplatte wird vor dem Einbau in einen HP Computer mittels DPS getestet. Dabei werden wichtige Informationen auf der Festplatte gespeichert. Die Testergebnisse werden bei jeder Ausführung von DPS auf der Festplatte gespeichert. Diese Informationen erleichtern dem Servicepartner eine Diagnose der Bedingungen, aufgrund derer Sie DPS ausgeführt haben. Weitere Informationen zur Verwendung von DPS finden Sie im *Fehlerbeseitigungs-Handbuch* auf der *Documentation and Diagnostics CD*.

Überspannungsschutz

Durch ein integriertes überspannungstolerantes Netzteil wird eine größere Zuverlässigkeit erzielt, wenn der Computer Spannungsspitzen ausgesetzt wird. Dieses Netzteil ist so ausgelegt, dass eine Überspannung von bis zu 2.000 V ohne Systemausfall oder Datenverluste neutralisiert werden kann.

Thermosensor

Der Thermosensor ist eine Hard- und Softwarefunktion zur Messung der Innentemperatur eines Computers. Diese Funktion zeigt eine Warnmeldung an, wenn der normale Temperaturbereich überschritten wird. Auf diese Weise können Sie Maßnahmen ergreifen, bevor die internen Komponenten beschädigt werden oder Daten verloren gehen.

Index